REMARKS

Please reconsider the present application in view of the above amendments and following remarks. Applicant thanks Examiner for carefully considering the present application.

Claims 1-32 are currently pending. By way of this reply, the specification is amended, and claims 1, 7, 9, 12, 15-26, and 28-32 are amended.

Response to Priority Claim

In the 2nd paragraph of the Non-Final Office Action, Examiner noted that "for benefit claims under 35 U.S.C. 120, 121, or 365(c), the reference must include the relationship (i.e., continuation, divisional, or continuation-in-part) of the applications." The specification is amended to specify that the present application is a continuation-in-part of U.S. Patent Application Serial No. 10/612,198.

Response to Claim Objections

In the 3rd paragraph of the Non-Final Office Action, Examiner objected to claims 1-32 because of informalities. Specifically, Examiner noted that some claims use the preposition "said" and some other claims use the preposition "the." To address this concern, the claims have been amended to replace the preposition "said" with "the." Examiner also noted that claim 19 uses "real-time," inconsistent with claim 16. Applicant respectively disagrees. Claim 16 does not contain "real time" or "real-time" in the claim language. Claims 8, 19, 20, 22, 23, and 27 use "real-time" as compound adjectives to describe how auditing is conducted. Claim 17 uses "real time" in a phrase "in real time" to describe how actions are performed. Because their roles are different, Applicant respectfully disagrees that the phrase "real time" in claim 17 is inconsistent with the compound adjective "real-time" in claims 8, 19, 20, 22, 23, and 27. Accordingly, Applicant respectfully requests that Examiner reconsider and withdraw the objections.

Response to Rejection Under 35 USC 101

In the 4th paragraph of the Non-Final Office Action, Examiner rejected claims 1-11 and 13-24 under 35 USC 101 as allegedly lacking useful results because "The flagged data as recited in the claim language is not further utilized in any particular way."

Applicant respectfully submits that the claimed invention has well-established useful results in flagging the retrieval command as suspicious. Nevertheless, to expedite prosecution Applicant has amended claims 1, 31, and 32 to include limitations similar to the limitations recited in claim 12, as suggested by Examiner. Accordingly, Applicant respectfully requests that Examiner reconsider and withdraw the rejection.

Response to Rejection Under 35 USC 112

In the 5th paragraph through the 9th paragraph of the Non-Final Office Action, Examiner rejected claims 1-32 under 35 USC 112 as allegedly "failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention." This rejection is traversed.

Examiner noted that the preambles in claims 1, 31, and 32 do not support the bodies of the claims. Applicant does not concede that the preambles in claims 1, 32, and 33 lack support for the bodies of the claims. Nevertheless, to expedite prosecution Applicant has amended independent claim 1 to recite "responsive to the retrieval command being not acceptable, performing at least one of the following: … restricting the retrieval command from accessing the computer code …." Independent claims 31 and 33 are similarly amended. Therefore, Applicant respectfully requests that Examiner reconsider and withdraw the rejection.

Examiner noted that Examiner was not able to ascertain the exact meaning of the term the term "canonicalized command" in claim 11. Examiner further noted that "For example it is not clear whether the command is a command that is some kind of executable code that changes a value to a 'wildcard' notation, whether it is a command the value of which is changed to a wildcard value or whether it is a command comprising a wildcard value." Applicant respectively disagrees. In page 7, lines 1-15 of the present application, the term "canonicalized command" is clearly defined as "a command stripped of its literal field data." The application further provided an example command "SELECT NAME FROM PATIENTS WHERE NAME LIKE 'FRANK' AND AGE > 25" and an example canonicalized command corresponding to the above example command "SELECT NAME FROM PATIENTS WHERE NAME LIKE * AND AGE > *". Therefore, a canonicalized command is a form of a command with its literal field data removed. It is not necessarily "a command that is some kind of executable code that changes a value to a 'wildcard' notation," nor "a command the value of which <u>is changed</u> to a wildcard value" (emphasis in original language), nor "a command comprising a wildcard value." The literal field data are removed, and not necessarily replaced by a wildcard. The above example uses '*' in place of the literal field data only to illustrate one way to remove a command's literal field data. Accordingly, Applicant respectfully requests that Examiner consider the claim language "canonicalized command" in light of the above argument for purpose of further examination.

Examiner noted that the phrase "training phase" is allegedly not understood and no clear definition was found in the specification. Specifically, Examiner suggested that "For purposes of further examination the examiner interprets the 'training phase' as phase during which a system operator (e.g. administrator) get familiar with the system (observes, updates, tests etc.)." Applicant respectfully notes that the phrase "training phase" is clearly defined in the specification with respect to figure 3. See page 3, lines 17 and 18 ("Figure 3 is a flow diagram illustrating a training phase of the present invention.") and page 16, line 1 through page 22, line 3. Training phase is a phase where a system observes retrieval commands (see page 16, lines 12-27 and figure 3) and responses, and updates a state table with retrieval information derived from the responses (see page 18, line 5-18 and figure 3). The system subsequently converts the retrieval information stored in the state table into rules for determining acceptable and/or unacceptable retrieval commands. See page 20, lines 16-19. Therefore, training phase is a phase for the system to observe and compile retrieval information, not a "phase during which a system operator (e.g. administrator) get familiar with the system (observes, updates, tests etc.)." Accordingly, Applicant respectfully requests that Examiner consider the claim language "training phase" in light of the above argument for purpose of further examination.

Response to Rejection Under 35 USC 102(e) or 103(a) in View of Mattsson

In the 10th paragraph through 13th paragraph of the Non-Final Office Action, Examiner rejected claims 1-8, 10, 12, 13, 27, and 30-32 under 35 USC § 102(e) as allegedly being anticipated by or, in the alternative, under 35 USC § 103(a) as obvious over U.S. Patent No. 7,120,933 to Mattsson ("Mattsson"). In the 14th paragraph through 19th paragraph of the Non-Final Office Action, Examiner rejected claims 9, 11, 14, 28, and 29 under 35 USC § 103(a) as obvious over Mattsson. For the reasons set forth below, these rejections are respectfully traversed.

Independent claim 1 as amended recites:

> A computer-implemented method for protecting computer code from malicious retrievers, the method comprising the steps of:
>
> observing a plurality of retrieval commands that access the computer code;
>
> observing responses to the plurality of retrieval commands generated by the computer code;
>
> **deriving from the plurality of retrieval commands and the responses a set of retrieval information, the set of retrieval information comprising input vectors characterizing the plurality of retrieval commands;**
>
> **converting the set of retrieval information into at least one rule for determining whether retrieval commands are acceptable;** .... (emphasis added)

Therefore, independent claim 1 as amended beneficially recites a method for protecting computer code from malicious retrievers by deriving from a plurality of retrieval commands and corresponding responses a set of retrieval information containing input vectors characterizing the plurality of retrieval commands, and converting the set of retrieval information into at least one rule. The at least one rule is subsequently used to determine whether a retrieval command is acceptable. Thus, the claimed method beneficially creates rules for determining whether a retrieval command is acceptable based on retrieval information derived from observed retrieval commands and responses. Independent claims 31 and 32 as amended recite similar features.

Mattsson, among other differences, does not disclose deriving from a plurality of retrieval commands and corresponding responses a set of retrieval information containing input vectors characterizing the plurality of retrieval commands, or converting the set of retrieval information into at least one rule for determining whether a retrieval command is acceptable. Mattsson, in contrast, discloses a method for detecting intrusion in a database by analyzing query results with item access rates included in security policies. See Mattsson, Summary and col. 4, lines 35-59. Mattsson merely discloses storing query results in a record to determine whether the query results exceed a particular item access rate. See Mattsson, col. 4, lines 35-59. This is different from the claimed invention because the query results do not contain "input vectors characterizing the plurality of retrieval commands" as claimed in independent claim 1. Mattsson suggests that a server has access to a plurality of security policies that can be stored in a security administration system, but is totally silent as to how the security policies are created. See Mattsson, col. 3, lines 51-57. Therefore, Mattsson also fails to disclose "converting the set of retrieval information into at least one rule for determining whether retrieval commands are acceptable."

In view of the above, Mattsson fails to disclose each and every limitation recited in independent claims 1, 31, and 32. Thus, independent claims 1, 31, and 32 are patentably distinguishable over the cited reference. The dependent claims are allowable for at least the same reason. Accordingly, withdrawal of the rejections under § 102 or § 103 in View of Mattsson is respectfully requested.

Response to Rejection Under 35 USC 103(a) in View of Mattsson and Sekar

In the 20th paragraph through 26th paragraph of the Non-Final Office Action, Examiner rejected claims 15-26 under 35 USC § 103(a) as obvious over Mattsson in view of

U.S. Publication 2004/0098617 A1 to Sekar ("Sekar"). For the reasons set forth below, these rejections are respectfully traversed.

As discussed above, Mattsson fails to disclose "deriving from the plurality of retrieval commands and the responses a set of retrieval information, the set of retrieval information comprising input vectors characterizing the plurality of retrieval commands; converting the set of retrieval information into at least one rule for determining whether retrieval commands are acceptable" as claimed in independent claim 1.

Sekar similarly fails to disclose the above cited claim elements. Sekar, in contrast, discloses a method for network intrusion detection on a network. See Sekar, Summary. Sekar discloses a system that can be run in a training mode wherein a state machine can be used to follow the processing of network packets. The system determines statistics for properties associated with the state machine transitions during the training mode and compares the determined statistics to statistics observed for subsequent network packets. If a determined statistical property of subsequent network packets deviates significantly from the statistics of the statistical property determined during the training mode, the system generates an alarm. See Sekar, paragraphs [0006], [0032], and [0097]. Sekar merely discloses determining "statistics associated with state machine transitions" and is totally silent as to "deriving from the plurality of retrieval commands and the responses a set of retrieval information, the set of retrieval information comprising input vectors characterizing the plurality of retrieval commands." The input vector is different from the "statistics associated with state machine transitions" because it may contain information that may not be described in statistics, such as logins of users, fields or combination of fields being accessed by a given retrieval command, and so on. Sekar also fails to disclose "converting the set of retrieval information into at least one rule for determining whether retrieval commands are acceptable." The statistics determined in Sekar are used to compare with subsequent statistical property, and not to convert "into at least one rule for determining whether retrieval commands are acceptable" as is claimed in independent claim 1.

In view of the above, Mattsson and Sekar, whether considered individually or in combination, fail to disclose each and every limitation recited in independent claims 1, 31, and 32. Thus, independent claims 1, 31, and 32 are patentable over Mattsson and Sekar. Dependent claims are allowable for at least the same reasons. Accordingly, withdrawal of the § 103 rejections is respectfully requested.

Conclusion

In sum, Applicant respectfully submits that claims 1-32, as presented herein, are patentably distinguishable over the cited references. Therefore, Applicant requests reconsideration of the basis for the rejections to these claims and requests allowance of them.

In addition, Applicant respectfully invites Examiner to contact Applicant's representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
Carey Nachenberg

Date: July 4, 2007 By: /Jie Zhang/

Jie Zhang, Reg. No. 60,242
Attorney for Applicant
Fenwick & West LLP
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7297
Fax: (650) 938-5200